

REMARKS

Favorable consideration of this Application as presently amended, and in light of the following discussion is respectfully requested.

Claims 11-20, 22-29, 38-44, and 50-52 are pending in the application; Claims 11 and 50 are amended; Claims 51-52 are added; and Claims 1-5 and 21 are canceled by the present amendment. Support for amended Claim 11, and new Claims 51-52 can be found in the original specification, claims and drawings.<sup>1</sup> No new matter is presented.

In the outstanding Official Action, Claims 1, 11 and 21 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite; Claims 1-5, 11-22, 25-29, 38-44 and 50 were rejected under 35 U.S.C. § 103 as unpatentable over Zhang et al. (U.S. Patent No. 6,550,008, hereinafter “Zhang”) in view of Sims III (U.S. Pub. No. 2002/0016919, hereinafter “Sims”); and Claims 23-24 were rejected under 35 U.S.C. § 103 as unpatentable over Zhang and Sims in view of Yagawa et al. (U.S. Patent No. 6,751,598, hereinafter “Yagawa”).

The Official Action rejected Claims 1, 11 and 21 under 35 U.S.C. § 112, second paragraph, as indefinite, asserting that the phrase “before said contents is transmitted/received” had insufficient antecedent basis. In response, Claim 11 is amended to recite “before transmitting/receiving said first contents data” and “before transmitting/receiving said second contents data,” to rely on the prior recitation of “first contents data” and “second contents data” recited in amended Claim 11. Claims 1 and 11 are canceled.

Accordingly, Applicants respectfully request that the rejection of Claim 11 under 35 U.S.C. § 112, second paragraph, be withdrawn.

The Official Action rejected Claims 1-5, 11-22, 25-29, 38-44 and 50 under 35 U.S.C. § 103 as unpatentable over Zhang in view of Sims. Applicants respectfully submit that

---

<sup>1</sup> e.g. specification, Fig. 4, and original Claim 1.

independent Claims 11, 22, 38-39 and 50 state novel features clearly not taught or rendered obvious by the applied references, and that there is insufficient motivation or suggestion to combine the cited references to arrive at Applicant's claims.

Amended independent Claim 11 relates to a method for furnishing key data to a data processing apparatus (e.g., a personal computer), which includes a contents reproducing program. The data processing apparatus receives a first key used to acquire first contents data from a compact disc, which is stored in the data processing apparatus. The first key is also used to perform authentication between the data processing apparatus and a portable reproducing apparatus (e.g., portable media player), thereby allowing for the first contents data to be exchanged between the two devices. The data processing apparatus also receives second key data that is used to acquire second contents data from a contents server, which is stored in the data processing apparatus. Similar to the first key, the second key is used to perform authentication between the data processing apparatus and a portable reproducing apparatus (e.g., portable media player), thereby allowing for the second contents data to be exchanged between the two devices.

The system of Claim 1 allows for increased security relating to content data downloaded from the content server by utilizing key data, different from the key data used for data from a conventional compact disc, when exchanging data between the data processing apparatus and the portable reproducing apparatus.

Independent Claims 22, 38, 39, 50 and 51, while directed to alternative components of the method recited in independent Claim 1, recite substantially similar subject matter.

Accordingly, the discussion below is also applicable to these claims.

Turning to the applied reference, Zhang describes a method for protecting information transmitted between a POD module (26) and a host device (24), which are both included in a

receiver (20) for receiving content data broadcast from a head end system (14).<sup>2</sup> Zhang's system, however, operates in a fundamentally different manner than the method recited in amended Claim 11, and therefore, Zhang fails to teach or suggest specific features recited in amended Claim 11.

Amended Claim 11 recites, *inter alia*, a contents purveying system including a data processor, wherein

***...using said first key data to acquire first contents data stored in a compact disc for storage in said data processing apparatus, and using said first key data to perform authentication between said data processing apparatus and a portable reproducing apparatus*** connected to said data processing apparatus before transmitting/receiving said first contents data between said data processing apparatus and said portable reproducing apparatus...

***using said second key data to acquire the second contents data furnished from said contents server for storage in said data processing apparatus, said second key data also being used to perform authentication between said data processing apparatus and said portable reproducing apparatus*** before transmitting/receiving said second contents data between said data processing apparatus and said portable reproducing apparatus.

As an initial matter, Applicants wish to point out the inconsistency in construing either the host device or the POD module as a “portable reproducing device,” in the context of the present claims. As shown in Figs. 1A-1B, the POD module and host device are configured to be two devices located in the same television signal receiver.<sup>3</sup> A cable television receiver is clearly not a portable device, and moreover, it would be unreasonable to consider either the POD device or host device located therein to individually be portable devices, since the receiver of Zhang does not function properly without both the POD device and the host device. Accordingly, Applicants submit that Zhang fails to teach or suggest the use of a “portable reproduction device,” whatsoever.

---

<sup>2</sup> Zhang, Fig. 1.

<sup>3</sup> Id., col. 2, lines 49-65.

Nonetheless, Applicants wish to reiterate that, while Zhang may assert that the POD module and host device are interchangeable, as discussed in the Advisory Action of August 31, 2005, Zhang's description is clear regarding the role each of these components satisfies in his system. Accordingly, for the remarks that follow, the POD module is discussed in relation to the "data processing apparatus" recited in amended Claim 11, and the host device will be discussed in relation to the "portable reproducing device", as recited in amended Claim 11. Any interpretation to the contrary is an unreasonable interpretation of the claims and/or Zhang's system, and it would not be possible for Zhang's system to properly function without the POD module and host device performing their respective roles, as specified in Zhang's specification. While Applicants acknowledge that the hardware and software components of the POD module and host device may be interchangeable, their assigned functions for the proper operation of Zhang's are not.

The outstanding Official Action asserts that col. 3, lines 45-65 and col. 11, lines 28-35 of Zhang discloses "furnishing a first key to said data processing apparatus." This cited portion of Zhang describes a process of verifying the identities of the POD module and the host device based on special binding messages, which are transmitted by the head-end system. Using these messages from the head-end system, the POD module and the host device can generate a session key for encrypting and decrypting messages transmitted between the POD module and the host device. Thus, the Official Action clearly asserts that the session key used between the POD module and host device corresponds to the furnished "first key," as recited in amended Claim 11.

Amended Claim 11 also recites that this "***first key***" is used "***to acquire first contents data stored in a compact disc for storage in said data processing apparatus.***" In addressing this claimed feature the Official Action cites col. 7, lines 15-30 and 45-51 of Zhang. This cited portion of Zhang describes that storage elements (e.g., including a compact disc) may

be included in the POD or host device for storing information such as authorization fields, binding message from the head-end system, transmitted content from the head end system, etc. The reference also discusses that sensitive information may be kept in the storage elements, and external access thereto is prevented. As admitted in the Official Action, however, Zhang fails to teach or suggest that either the POD device or host device use the session key to access any information from an attached storage medium, whatsoever. Specifically the Official Action admits that Zhang is “silent about the POD retrieving the data from the storage element because it is obvious that if data is stored on in the CD it must be retrieved using a key.”<sup>4</sup>

In an attempt to cure this deficiency in Zhang, the Official Action relies on Sims, citing p. 8, paragraph [0081] and p. 9, paragraph [0098]. Sims, however, is directed to using a key (e.g., Disk Key) for ensuring that a specific device or user is authorized to access the content stored in a bulk media storage. In paragraph [0083], Sims describes that decryption values (e.g., p, q, e and k), as well as other information, is provided to authorized users which are operable to receive and decrypt given content data.

However, as noted above, the Official Action asserts that the “first key,” as claimed, is analogous to the session key generated between the POD device and the host device for authentication. Claim 11 also recites that this “***first key***” is used “***to acquire first contents data stored in a compact disc for storage in said data processing apparatus.***” Sims, in contrast to both Zhang and the present claims, describes that the key used to obtain data from the bulk media storage is included in the bulk media storage and exchanged accordingly with authorized devices. Thus, this “first key,” which the Official Action states is analogous to the session key, discussed above, is not used to “***to acquire first contents data stored in a compact disc for storage in said data processing apparatus,***” whatsoever.

---

<sup>4</sup> Outstanding Official Action, p. 5.

Further, the “Disc Key” of Sims is not interchangeable with the session key generated by Zhang, and therefore they both can not be considered the claimed “first key.” As discussed above, Zhang uses a very specific authentication/binding process involving the head end to generate a session key for the exchange of data between the host device and the POD. In contrast, Sims describes a process for embedding the key in the bulk media storage and only exchanging this key data with authorized users or media devices. Therefore, the process for generating the keys in the two references is completely different, and combining the methods of Zhang and Sims to use the same key for both authentication between the two devices, and for obtaining data from the bulk media storage medium would appear to necessitate a substantial redesign of Zhang’s system. Further, due to the inconsistencies between the key processes in the two methods devices, it would appear that the Official Action’s attempt to bring the isolated teachings of Sims’ method into Zhang’s method would amount to improperly picking and choosing features without regard to the teachings of the references as a whole.<sup>5</sup>

Thus, there is no motivation or suggestion, whatsoever, to combine the Zhang and Sims references and assert that the “Disc Key” of Sims, and the session key of Zhang, may each be considered the “first key,” as recited in amended independent Claim 11, for the reasons noted above. While the required evidence of motivation to combine need not come from the applied references themselves, the evidence must come from *somewhere* within the record.<sup>6</sup> In this case, the record fails to support the proposed modification of Zhang.

---

<sup>5</sup> See In re Ehrreich 590 F2d 902, 200 USPQ 504 (CCPA, 1979) (stating that patentability must be addressed “in terms of what would have been obvious to one of ordinary skill in the art at the time the invention was made in view of the sum of all the relevant teachings in the art, not in view of first one and then another of the isolated teachings in the art,” and that one “must consider the entirety of the disclosure made by the references, and avoid combining them indiscriminately.”)

<sup>6</sup> In re Lee, 277 F.3d 1338, 1343-4, 61 USPQ2d 1430 (Fed. Cir. 2002) (“The factual inquiry whether to combine references ... must be based on objective evidence of record. ... [The] factual question of motivation ... cannot be resolved on subjective belief and unknown authority. ... Thus, the Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency’s conclusion”).

Amended Claim 11 also recites, “*using said second key data to acquire the second contents data furnished from said contents server,*” and “*said second key data also being used to perform authentication between said data processing apparatus and said portable reproducing apparatus.*” Thus, the contents data is acquired by the data processing apparatus using second key data, and before transmitting the content from the data processor to the portable reproducing device, authentication is performed using the same second key data for storage between the data processor and the portable reproducing device.

Zhang, however, fails to teach or suggest receiving second key data over a network at the POD module, and using the second master key to both obtain data over the network and perform authentication with the host device. As discussed above, Zhang describes that the POD module and host device generate a session key to exchange content data based on the binding messages received from the head-end unit. However, this session key is not the same as the “conditional access protocol” encryption used to receive and decrypt the information received at the POD module from the head-end unit (asserted in the Official Action as analogous to the “contents server”).<sup>7</sup> Thus, while Zhang describes that information is retrieved from the head-end unit that allows the POD module and host device to perform mutual authentication and generate a session key, this session key used to exchange contents is not the same as the key used by the POD module to retrieve and decrypt content received from the head-end unit. Therefore, Zhang fails to teach or suggest using a second master key for storage for both acquiring data from a contents server and performing authentication between the data processor and the portable reproduction device.

The Official Action also asserts that “it would have been obvious to one skilled at the art at the time of the invention was made to modify the invention of Zhang et al. to use

---

<sup>7</sup> Id., col. 10, lines 18-29.

public/private key scheme for encrypting data instead of generating symmetric key data in the device as public/private key provides more security.”<sup>8</sup> However, the Official Action fails to provide any support why the use of a public/private key would provide greater security than the already implemented method of Zhang, discussed above. Zhang already describes that his design achieves the objective of exchanging data in secure manner by using the “conditional access protocol” encryption to receive and decrypt the information received at the POD module from the head-end unit (asserted in the Official Action as analogous to the “contents server”).<sup>9</sup> The session key is then used to exchange the content data, if necessary, with the host device. Thus, since Zhang’s device uses two separate keys (one for authentication with the host device, and one for reception from the head end), it would clearly have an additional level of security, and thus be more secure than using the same public/private key for both downloading the data from the head end and authenticating with the host device. Accordingly, there is no motivation or suggestion, whatsoever, to incorporate the use of a public/private key scheme to both receive data from the head end and authenticate the POD device with the host device, as this would appear to require a substantial redesign of Zhang’s system, and also decrease the security in the system.

Further, while the Official Action states that the public/private key scheme could be used for encryption decryption of content data, it fails to assert how such a system would be used to perform authentication between the POD device and host device of Zhang. Thus, the proposed modification, even if appropriate, fails to teach or suggest all the features recited in amended independent Claim 11.

Thus, Zhang fails to teach or suggest, *inter alia*, “**using said second key data to acquire the second contents data furnished from said contents server,**” and “**said second**

---

<sup>8</sup> Outstanding Official Action., p.5.

<sup>9</sup> Id., col. 10, lines 18-29.



***key data also being used to perform authentication between said data processing apparatus and said portable reproducing apparatus,”*** as recited in amended independent Claim 11.

Accordingly, for at least the reasons discussed above, Applicants respectfully request that the rejection of Claim 11 under 35 U.S.C. § 103 as unpatentable over Zhang and/or Sims be withdrawn. For substantially the same reasons as given with respect to amended Claim 11, it is also submitted that amended independent Claims 21, 38, 39, 50 and 51 also patentably define over the applied references.

The Official Action has rejected Claims 23 and 24 under 35 U.S.C. § 103 as being unpatentable over Zhang and Sims in view of Yagawa.

As discussed above, neither Zhang, nor Sims, alone or in combination fails to teach or suggest specific above-noted features recited in the pending independent Claims. Likewise Yagawa fails to remedy this deficiency, and therefore, none of the cited references, either alone or in combination, can be asserted as disclosing Applicants Claims 23 and 24, which include the above distinguished limitation by virtue of dependency. Therefore the Official Action does not provide a *prima facie* case of obviousness with regard to any of these claims.

Accordingly, Applicant respectfully requests that the rejection of Claims 23 and 24 under 35 U.S.C. § 103 be withdrawn.

Application No. 09/857,218  
Reply to Office Action of December 29, 2005

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by Claims 11-20, 22-29, 38-44, and 50-52 is definite and patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

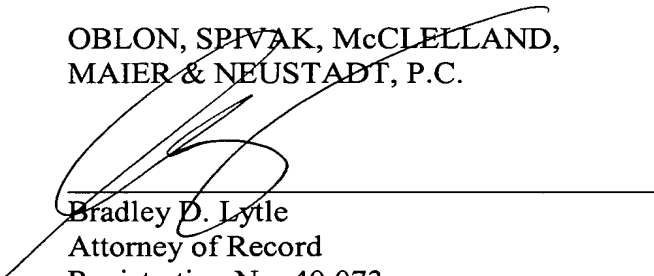
Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Customer Number

**22850**

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 06/04)



---

Bradley D. Lytle  
Attorney of Record  
Registration No. 40,073  
Andrew T. Harry  
Registration No. 56,959

BDL/ATH/kkn

I:\ATTY\ATH\PROSECUTION\20'S\209462-US\209462.AM DUE MARCH 29..DOC